

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

01/14/2015

SUBJECT:

Multiple Vulnerabilities in Mozilla Firefox, Thunderbird, and SeaMonkey Could Allow for Remote Code Execution

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been identified in Mozilla Firefox and Thunderbird which could allow for remote code execution. Mozilla Firefox is a web browser used to access the Internet and Mozilla Thunderbird is an email client. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

Mozilla Firefox versions prior to 35

Mozilla Firefox Extended Support Release (ESR) version prior to 31.4

Mozilla Thunderbird versions prior to 31.4

SeaMonkey versions prior to 2.32

RISK:

Government:

Large and medium government entities: **High**

Small government entities: **High**

Businesses:

Large and medium business entities: **High**

Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Ten vulnerabilities have been reported in Mozilla Firefox, Thunderbird, and SeaMonkey. Details of the vulnerabilities are as follows:

Mozilla Firefox, Thunderbird, and SeaMonkey are prone to multiple miscellaneous memory safety vulnerabilities that exist in the browser engine. [CVE-2014-8634, CVE-2014-8635, MFSa 2015-01]

Mozilla Firefox is prone to an uninitialized memory use vulnerability when processing specially crafted bitmap images [CVE-2014-8637, MFSa 2015-02]

Mozilla Firefox, Thunderbird, and SeaMonkey are prone to a cross-site request forgery vulnerability when passing a sendBeacon request because it lacks an origin header. [CVE-2014-8638, MFSa 2015-03]

Mozilla Firefox, Thunderbird, and SeaMonkey are prone to a cookie injection vulnerability. [CVE-2014-8639, MFSa 2015-04]

Mozilla Firefox is prone to a read of uninitialized memory vulnerability in Web Audio. This vulnerability causes the browser to crash. [CVE-2014-8640, MFSa 2015-05]

Mozilla Firefox is prone to a read-after-free vulnerability in WebRTC due to the way that tracks are handled. This results in a potentially exploitable crash. [CVE-2014-8641, MFSa 2015-06]

Mozilla Firefox is prone to a security vulnerability which allows for an escape from the Gecko Media Plugin sandbox on Windows systems. [CVE-2014-8643, MFSa 2015-07]

Mozilla Firefox is prone to a security vulnerability that could allow for users to connect to a site with a revoke certificate. [CVE-2014-8642, MFSa 2015-08]

Mozilla Firefox is prone to a security bypass vulnerability which could allow for specially crafted Document Object Model (DOM) objects to bypass XrayWrappers and potentially enable privilege escalation. [CVE-2014-8636, MFSa 2015-09]

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Mozilla to vulnerable systems immediately after appropriate testing.

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

- Remind users not to click links from unknown sources, or to click links without verifying the intended destination.

REFERENCES:

Mozilla:

<https://www.mozilla.org/en-US/security/advisories/mfsa2015-01/>

<https://www.mozilla.org/en-US/security/advisories/mfsa2015-02/>

<https://www.mozilla.org/en-US/security/advisories/mfsa2015-03/>

<https://www.mozilla.org/en-US/security/advisories/mfsa2015-04/>

<https://www.mozilla.org/en-US/security/advisories/mfsa2015-05/>

<https://www.mozilla.org/en-US/security/advisories/mfsa2015-06/>

<https://www.mozilla.org/en-US/security/advisories/mfsa2015-07/>

<https://www.mozilla.org/en-US/security/advisories/mfsa2015-08/>

<https://www.mozilla.org/en-US/security/advisories/mfsa2015-09/>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8634>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8635>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8636>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8637>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8638>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8639>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8640>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8641>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8642>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8643>

Security Focus:

<http://www.securityfocus.com/bid/72041>
<http://www.securityfocus.com/bid/72042>
<http://www.securityfocus.com/bid/72043>
<http://www.securityfocus.com/bid/72044>
<http://www.securityfocus.com/bid/72045>
<http://www.securityfocus.com/bid/72046>
<http://www.securityfocus.com/bid/72047>
<http://www.securityfocus.com/bid/72048>
<http://www.securityfocus.com/bid/72049>
<http://www.securityfocus.com/bid/72050>